530,203

Rec'd PCT/PTO 04 APR 2005

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

10/530203

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
15 avril 2004 (15.04.2004)

PCT

(10) Numéro de publication internationale
WO 2004/032042 A1

(51) Classification internationale des brevets[7] : G06K 19/07

(21) Numéro de la demande internationale : PCT/FR2003/002854

(22) Date de dépôt international : 29 septembre 2003 (29.09.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/12340 4 octobre 2002 (04.10.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **OBERTHUR CARD SYSTEMS SA** [FR/FR]; 102, boulevard Malesherbes, F-75017 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **JAYET, Stéphane** [FR/FR]; 25, allée des Noisetiers, F-95250 Beauchamp (FR). **HUOT, Jean-Claude** [FR/FR]; 14, rue Hoche, F-78350 Jouy-en-Josas (FR).

(74) Mandataire : **SANTARELLI**; 14, avenue de la Grande Armée, Boîte postale 237, F-75822 Paris Cedex 17 (FR).

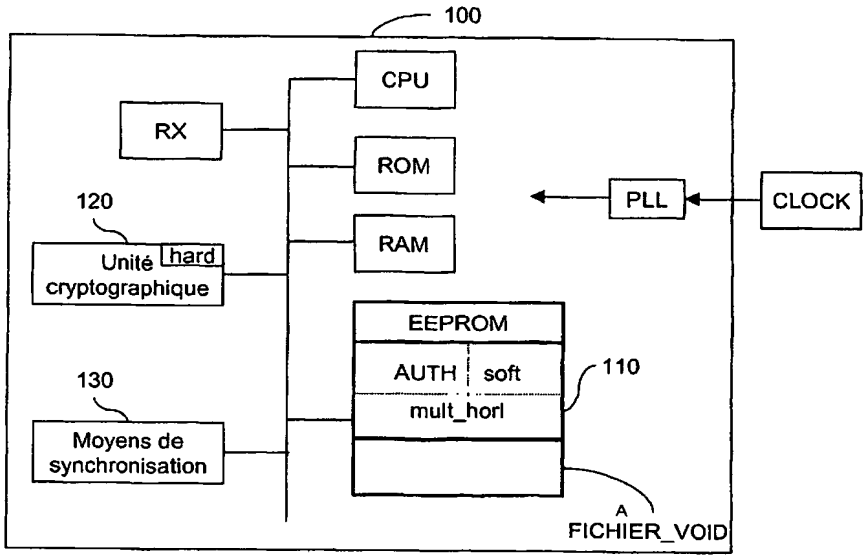
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet

[Suite sur la page suivante]

(54) Title: MICROCIRCUIT CARD WHEREOF THE PERFORMANCES CAN BE MODIFIED AFTER CUSTOMIZATION

(54) Titre : CARTE A MICROCIRCUIT DONT LES PERFORMANCES PEUVENT ETRE MODIFIEES APRES PERSONNALISATION



120...CRYPTOGRAPHIC UNIT
130...SYNCHRONIZATION MEANS
A...FILE_VOID

(57) Abstract: The invention concerns a microcircuit card comprising means (RX) for receiving a command and means for modifying at least one performance of the card capable of being implemented after a step of customization of the card.

[Suite sur la page suivante]

WO 2004/032042 A1

européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : Cette carte à microcircuit comprend des moyens (RX) de réception d'une commande et des moyens de modification d'au moins une performance de la carte pouvant être mis en oeuvre après une étape de personnalisation de la carte.

Carte à microcircuit dont les performances peuvent être modifiées après personnalisation

La présente invention concerne une carte à microcircuit dont les performances peuvent être modifiées après une étape de personnalisation de la carte, et un procédé de configuration d'une telle carte.

Dans la suite de ce document, le terme *"personnalisation"* (ou individualisation) sera compris comme étant celui utilisé couramment par l'homme du métier dans l'industrie des cartes à microcircuit, ou tel que défini par W.Rankl et W.Effing dans le document *"Smart Card Handbook, Second Edition, Ed. John Wiley & Sons, Ltd"* de la façon suivante :

"Le terme personnalisation, dans son sens le plus large, signifie que les données spécifiques à une carte ou à une personne sont entrées dans la carte. Ces données peuvent par exemple être un nom, une adresse, mais aussi des clefs associées à la carte. La seule chose qui importe est que ces données soient spécifiques à cette carte."

L'invention trouve une application privilégiée, mais non limitative, dans le domaine des cartes à microcircuit de télécommunication mobile telles que les cartes SIM conformes à la norme GSM ou des cartes conformes à des normes similaires telles que les normes CDMA, TDMA ou UMTS. Dans ce contexte, l'invention permet la modification des performances d'une carte de télécommunication mobile personnalisée et déjà attribuée à un utilisateur abonné à un service de téléphonie mobile.

La modification de la fréquence d'horloge d'une carte à microcircuit est déjà connue de l'homme du métier lorsqu'elle s'effectue avant l'étape de personnalisation de la carte.

Un tel procédé est en particulier utilisé pendant les phases de développement d'une carte à microcircuit, phases au cours desquelles les cartes sont testées avec différentes fréquences d'horloge, la fréquence d'horloge de la carte étant ensuite figée avant la fin de la personnalisation.

Néanmoins, selon l'art antérieur, la modification des performances de la carte ne peut se faire après la personnalisation de la carte.

Il serait pourtant souhaitable de pouvoir modifier les performances d'une carte à microcircuit après personnalisation, notamment après sa commercialisation, ou plus généralement après qu'elle a été attribuée à un utilisateur.

A cet effet, l'invention concerne une carte à microcircuit comportant des moyens de réception d'une commande et des moyens de modification d'au moins une performance de la carte sur réception de la commande, les moyens de modification pouvant être mis en œuvre après une étape de personnalisation de la carte.

Corrélativement, l'invention vise, selon un deuxième aspect, un procédé de configuration d'une carte à microcircuit comportant les étapes successives suivantes :

- personnalisation de la carte ;
- réception d'une commande ; et
- modification d'au moins une performance de la carte sur réception de la commande.

Dans le contexte de la présente invention, une performance d'une carte à microcircuit pouvant être modifiée par un procédé de configuration conformément à la présente invention doit être comprise comme étant toute caractéristique matérielle ou logicielle préexistant dans la carte et non accessible après personnalisation.

L'invention permet ainsi d'améliorer ou de dégrader une performance d'une carte à microcircuit par l'envoi de la commande précitée après personnalisation, la carte étant déjà attribuée à un utilisateur. Sans la présente invention en revanche, un utilisateur souhaitant utiliser une carte avec des performances nouvelles doit nécessairement changer de carte à microcircuit.

Ainsi, l'utilisateur d'une carte à microcircuit comportant une mémoire physique EEPROM de 64 kilo-octets mais dont la taille de la zone utilisable a été limitée à 32 kilo-octets avant personnalisation, peut, sur

réception de la commande, bénéficier de la totalité des 64 kilo-octets de la mémoire physique sans avoir à changer de carte.

Selon une caractéristique avantageuse, la carte à microcircuit comporte en outre des moyens d'authentification d'un émetteur de la commande.

Dans un mode préféré de réalisation, ces moyens d'authentification comportent des moyens cryptographiques permettant de vérifier si la commande a été cryptée avec une clef d'authentification prédéterminée.

Ces moyens de vérification peuvent utiliser une fonction de hachage selon un algorithme du type MD4, MD5 ou SHA-1.

Ainsi, selon cette caractéristique avantageuse, les modifications de performance de la carte nécessitent la connaissance de la clef d'authentification, cette clef pouvant être gardée secrète par un opérateur, le fabricant de la carte ou tout tiers qui se réserve ainsi la possibilité de modifier les performances de la carte.

Dans une variante de réalisation, la clef d'authentification précitée est associée à la modification d'une performance prédéterminée d'une carte prédéterminée.

Selon une autre caractéristique, les moyens de modification sont adaptés à déterminer quelle performance de la carte doit être modifiée en fonction d'un ordre prédéterminé reçu dans la commande.

Cette caractéristique permet, selon l'ordre prédéterminé reçu dans la commande, de modifier une ou plusieurs caractéristiques de la carte.

Selon un mode de réalisation particulièrement avantageux, les moyens de réception sont adaptés à recevoir la commande selon le protocole SMS ou similaire tel que le protocole MMS (multimedia service).

Ce mode de réalisation permet ainsi la modification d'au moins une performance de la carte à travers un réseau de télécommunication mobile.

Bien entendu, dans d'autres modes de réalisation, la commande peut être reçue par les moyens de réception à travers un réseau filaire ou localement.

Selon un mode de réalisation préféré de la carte selon l'invention, les moyens de modification sont adaptés à modifier la taille d'une zone utilisable d'une mémoire physique de la carte.

Cette caractéristique permet ainsi d'augmenter les capacités de mémorisation de la carte, par exemple pour permettre le téléchargement de nouvelles applications dans la carte.

Dans une variante préférée de ce mode de réalisation, la modification de la taille de la zone utilisable de la mémoire physique est effectuée en créant ou en détruisant au moins un fichier spécifique compris dans la mémoire physique, ou en modifiant la taille d'au moins un fichier spécifique compris dans la mémoire physique.

Ce fichier peut être un fichier spécifiquement créé pour occuper un espace de la mémoire physique ou un fichier de données utilisé par une application de la carte à microcircuit.

Dans un autre mode de réalisation préféré, les moyens de modification d'au moins une performance sont adaptés à modifier, de façon réversible ou non une fréquence d'horloge de la carte.

Selon cette caractéristique particulière, on peut accélérer la vitesse de calcul d'un processeur ou d'un composant cryptographique de la carte, ce qui permet de réaliser des traitements plus complexes sur des données numériques reçues par la carte à microcircuit.

Dans un autre mode de réalisation, les moyens de modification d'au moins une performance sont adaptés à permettre ou empêcher, de façon réversible ou non, l'utilisation d'au moins une fonction logicielle de la carte.

Cette caractéristique particulière permet ainsi de valider des applications logicielles prévues initialement sur la carte mais invalidées avant la fin de sa personnalisation.

Une telle fonction logicielle peut par exemple être une fonction cryptographique telle qu'une fonction de contrôle d'une signature de données numériques.

De la même façon, dans un autre mode de réalisation, les moyens de modification de performance de la carte sont adaptés à permettre ou

empêcher, de façon réversible ou non, l'utilisation de tout ou partie d'un circuit électronique de la carte, ce circuit électronique pouvant par exemple être une unité cryptographique.

Les traitements cryptographiques qui étaient réalisés par logiciel peuvent ainsi avantageusement être accélérés par l'utilisation de cette unité cryptographique.

Dans un mode préféré de réalisation, la carte à microcircuit selon l'invention comporte en outre des moyens de synchronisation adaptés à vérifier l'unicité de la commande.

Cette caractéristique particulière permet avantageusement d'éviter une utilisation malhonnête de la carte à microcircuit en empêchant qu'une commande déjà reçue et copiée frauduleusement ne soit prise en compte une deuxième fois.

Les avantages et caractéristiques particulières propres au procédé de configuration selon l'invention étant similaires à ceux exposés ci-dessus concernant la carte à microcircuit conforme à l'invention, ils ne seront pas rappelés ici.

D'autres aspects et avantages de la présente invention apparaîtront plus clairement à la lecture des descriptions d'un mode particulier de réalisation qui va suivre cette description étant donnée à titre d'exemple non limitatif est faite en référence aux dessins annexés sur lesquels :

- la figure 1 représente de façon schématique l'architecture d'une carte à microcircuit conforme à l'invention ;
- la figure 2 représente une commande conforme à la présente invention, dans un mode préféré de réalisation ; et
- la figure 3 représente, sous forme d'organigramme, les principales étapes d'un procédé de configuration conforme à l'invention, dans un mode préféré de réalisation.

La **figure 1** représente de façon schématique l'architecture d'une carte à microcircuit 100 conforme à l'invention.

La carte à microcircuit 100 comporte principalement un processeur CPU associé de façon classique à un certain nombre de mémoires de type RAM, ROM et EEPROM.

La mémoire ROM comporte en particulier les instructions d'un programme informatique adapté à mettre en œuvre un procédé de configuration conforme à la présente invention et dont les principales étapes seront décrites ultérieurement en référence à la figure 3.

De même, la mémoire vive RAM comporte des registres nécessaires à l'exécution de ce programme.

La carte à microcircuit 100 comporte également une mémoire physique, par exemple une mémoire de type EEPROM, dont la taille d'une zone utilisable 110 peut être modifiée après personnalisation.

La carte à microcircuit 100 comporte également un circuit électronique 120, constitué dans le mode de réalisation décrit ici par une unité cryptographique.

De façon connue, la carte à microcircuit 100 reçoit également un signal d'une horloge CLOCK externe à la carte, ce signal d'horloge étant fourni aux différents composants de la carte.

Dans le mode de réalisation particulier décrit ici, la carte à microcircuit 100 comporte un composant de type PLL (Phase Lock Looping en anglais) connu de l'homme du métier et permettant de dériver des signaux à différentes fréquences d'horloge, à partir du signal de l'horloge externe CLOCK.

Plus précisément, dans le mode de réalisation décrit ici, la zone utilisable 110 de la mémoire EEPROM comporte un registre mult_horl pour mémoriser un facteur multiplicateur appliqué à la fréquence du signal de l'horloge externe CLOCK.

A la mise sous tension de la carte à microcircuit, le processeur CPU lit ce registre mult_horl et programme le composant PLL avec la valeur contenue dans ce registre, le signal d'horloge en sortie du composant PLL étant ensuite appliqué à certains composants de la carte.

Dans le mode de réalisation décrit ici, le composant PLL permet ainsi de modifier la vitesse de calcul du processeur CPU et de l'unité cryptographique 120.

La carte à microcircuit 100 selon l'invention comporte des moyens de réception RX d'une commande 200 qui va maintenant être décrite, dans un mode préféré de réalisation, en référence à la **figure 2**.

La commande 200 comporte un champ 210 comportant un ordre prédéterminé dont l'analyse permet de déterminer quelles sont les performances de la carte 100 qui doivent être modifiées.

Dans l'exemple de réalisation décrit ici, les performances de la carte à microcircuit 100 pouvant être modifiées après personnalisation sont, la taille de la zone utilisable 110 de la mémoire physique EEPROM, la fréquence du signal d'horloge, une fonction logicielle f mise en œuvre par le processeur CPU et le circuit électronique 120.

Dans le mode de réalisation préféré décrit ici, l'ordre 210 est constitué par un octet dont :

- le premier bit (bit1) et le deuxième bit (bit2) sont représentatifs d'un ordre de création ou de destruction d'une zone utilisable 110, ou d'un ordre de modification de la taille de la zone utilisable 110 de la mémoire physique EEPROM de la carte à microcircuit 100 ;
- le troisième (bit3) et le quatrième bit (bit4) constituent un facteur multiplicateur de la fréquence du signal d'horloge fourni par l'horloge externe CLOCK ;
- le cinquième bit (bit5) est représentatif d'un ordre d'utilisation ou de non utilisation d'une fonction logicielle f de la carte ;
- le sixième bit (bit6) est représentatif d'un ordre d'utilisation ou de non utilisation du circuit électronique 120 ; et
- les septième et huitième bits sont non utilisés.

Dans le mode préféré de réalisation décrit ici, les moyens de réception RX sont adaptés à recevoir la commande 200 selon le protocole SMS, par exemple au moyen de la commande ENVELOPE de ce protocole, et à mémoriser cette commande 200 dans une zone de la mémoire vive RAM.

La carte à microcircuit 100 comporte également des moyens d'authentification d'un émetteur de la commande 200.

Dans un mode préféré de réalisation, les moyens d'authentification comportent des moyens cryptographiques permettant de vérifier si la commande 200 a été cryptée avec une clef d'authentification AUTH prédéterminée, la clef d'authentification AUTH étant mémorisée dans une partie AUTH de la zone utilisable 110 de la mémoire EEPROM au moment de la personnalisation de la carte.

Ces moyens cryptographiques peuvent être constitués par un programme informatique exécuté par le processeur CPU, ce programme informatique comportant des instructions de mise en œuvre d'un algorithme de décryptage à clef publique tel que l'algorithme RSA connu de l'homme du métier.

Dans le mode préféré de réalisation décrit ici, la carte à microcircuit 100 comporte en outre des moyens de synchronisation 130 adaptés à vérifier l'unicité de la commande 200, de façon à éviter qu'une commande 200 déjà reçue et copiée frauduleusement ne soit prise en compte une deuxième fois de façon non autorisée.

Les moyens de synchronisation 130 peuvent en particulier être constitués par un circuit électronique mettant en œuvre le test E35 de vérification décrit ultérieurement en référence à la figure 3.

Selon un mode préféré de réalisation, le processeur CPU détermine, à partir de la commande 200, la ou les performances de la carte à microcircuit 100 qui doivent être modifiées.

En particulier, si le couplet (bit1, bit2) constitué par le premier bit bit1 et le deuxième bit bit2 de l'ordre 210 est égal à (1,1), cela signifie que la taille de la zone utilisable 110 de la mémoire physique EEPROM doit, si possible être augmentée.

En pratique, et dans le mode de réalisation préféré décrit ici, la carte à microcircuit 100 comporte, avant personnalisation, un fichier informatique FICHIER_VOID dans la mémoire physique EEPROM de telle sorte que lorsque le couplet (bit1, bit2) est égal à (1, 1), le processeur CPU détruit ce

fichier FICHIER_VOID libérant ainsi une partie de la mémoire physique EEPROM.

En variante, lorsque le couplet (bit1, bit2) est égal à (1,1), la taille de la zone utilisable de la mémoire physique EEPROM est (si possible) augmentée en diminuant la taille du fichier FICHIER_VOID de façon prédéterminée, par exemple de 16 kilo-octets.

De même, dans le mode préféré de réalisation décrit ici, lorsque le couplet (bit1, bit2) est égal à (0,0), cela signifie que la taille de la zone utilisable 110 de la mémoire physique EEPROM doit si possible être diminuée, cette opération étant réalisée en augmentant (si possible) la taille du fichier FICHIER_VOID de façon prédéterminée, par exemple de 16 kilo-octets.

En variante, lorsque le couplet (bit1, bit2) est égal à (0,0), cela signifie qu'un fichier FICHIER_VOID doit être créé, si possible, à une adresse et avec une taille prédéterminées dans la mémoire physique EEPROM.

Dans le mode de réalisation décrit ici, la réception d'une commande 200 dont le couplet (bit1, bit2) est égal à (1,0) ou (0,1) est sans effet.

Conformément à la norme ISO7816, la modification des caractéristiques (création, destruction, changement de taille) du fichier FICHIER_VOID peut nécessiter une clef CLEF spécifique 220 reçue dans la commande 200, tel que représenté à la figure 2.

Dans un autre mode préféré de réalisation, plusieurs fichiers du même type peuvent être prévus avant personnalisation de la carte, ce qui permet d'augmenter, progressivement, par destruction de ces fichiers la taille de la zone utilisable de la mémoire physique EEPROM.

D'autre part, lorsque la carte à microcircuit 100 reçoit l'ordre 210, le processeur CPU obtient, par lecture du troisième bit3 et quatrième bit4 bits de cet ordre 210, un facteur multiplicateur d'horloge.

Dans le mode préféré de réalisation décrit ici, ce facteur multiplicateur d'horloge est égal respectivement à 1, 2 et 3 pour les valeurs des couplets (bit3, bit4) respectivement égales à (0,1), (1,0), (1,1).

Dans le mode de réalisation particulier décrit ici, ce facteur multiplicateur est mémorisé dans le registre mult_horl de la zone utilisable 110 de la mémoire EEPROM, ce registre étant lu par le processeur CPU à la mise sous tension pour paramétrer le composant PLL.

Dans le mode de réalisation décrit ici, la carte à microcircuit comporte des moyens de modification adaptés à permettre ou à empêcher l'utilisation d'une fonction logicielle f de la carte.

En pratique, la mémoire morte ROM comporte un programme informatique pouvant invoquer cette fonction logicielle f lorsqu'un registre soft de la zone utilisable 110 de la mémoire non volatile EEPROM contient la valeur 1.

Sur réception de la commande 200, le processeur CPU lit, écrit dans le registre soft la valeur du cinquième bit bit5 de l'ordre prédéterminé reçu dans la commande 200.

Dans l'exemple décrit ici, la fonction logicielle est une fonction cryptographique ou une fonction de contrôle d'une signature de données numériques reçues par les moyens de réception RX.

La carte à microcircuit 100 comporte aussi des moyens de modification adaptés à permettre ou empêcher l'utilisation de tout ou partie d'un circuit électronique 120 de la carte.

Dans le mode de réalisation décrit ici, ce circuit électronique 120 comporte une unité cryptographique.

En pratique, l'utilisation de ce circuit électronique 120 est possible après écriture de la valeur 1 dans un registre hard de ce composant, la valeur de ce registre étant modifiée par le processeur CPU avec le contenu du sixième bit bit6 de l'ordre prédéterminé.

Dans l'exemple décrit ici, la modification de la fréquence d'horloge, l'autorisation ou l'empêchement d'utiliser la fonction logicielle ou le composant électronique sont des opérations réversibles. Dans un autre mode de réalisation, l'une au moins de ces opérations pourrait ne pas être réversible.

Nous allons maintenant décrire en référence à la **figure 3**, les principales étapes d'un procédé de configuration conforme à l'invention dans un mode préféré de réalisation.

Le procédé de configuration comporte une première étape E10 de personnalisation. Cette étape est connue de l'homme du métier, et ne sera décrite en détail ici.

Quoi qu'il en soit, cette étape de personnalisation consiste à écrire dans une mémoire de la carte, par exemple dans l'EEPROM des données spécifiques à cette carte ou à un utilisateur de cette carte.

Dans l'exemple décrit ici, cette étape de personnalisation comprend en particulier l'écriture dans une mémoire EEPROM de la carte à microcircuit 100 la valeur de la clef d'authentification AUTH.

Cette étape de personnalisation comprend aussi la création du fichier FICHIER_VOID et de sa clé 220 dans la mémoire EEPROM.

L'étape E10 est suivie par une étape E20 de réception de la commande 200 décrite précédemment en référence à la figure 2.

L'étape E20 est suivie par une étape de vérification E30 au cours de laquelle le processeur CPU authentifie un émetteur de la commande 200. Cette étape d'authentification s'effectue, dans le mode de réalisation décrit ici, en vérifiant si la commande 200 a été cryptée avec une clef d'authentification AUTH prédéterminée, la clef d'authentification AUTH étant mémorisée dans un registre de la mémoire EEPROM au moment de la personnalisation de la carte.

Si tel n'est pas le cas, le résultat du test E30 est négatif. Ce test est alors suivi par l'étape E20 de réception d'une commande déjà décrite.

En revanche, si l'émetteur de la commande 200 est authentifié comme autorisé à émettre la commande 200, le résultat du test E30 est positif.

Ce test est alors suivi par un test E35 au cours duquel on vérifie l'unicité de la commande 200. Ce test E35 de vérification permet d'éviter qu'une commande 200 déjà reçue et copiée frauduleusement ne soit prise en compte une deuxième fois de façon non autorisée.

De façon connue, ce test E35 de vérification peut être mis en œuvre en incorporant un numéro de message dans chaque commande 200, ce

numéro étant incrémenté pour chaque commande, et en comparant ce numéro reçu dans une commande 200 particulière, avec la valeur du numéro reçu dans la commande 200 précédente.

Si la commande 200 a déjà été reçue, le résultat du test de vérification E35 est négatif. Ce test est alors suivi par l'étape E20 de réception d'une commande 200 déjà décrite.

En revanche, si la commande 200 est reçue pour la première fois, le résultat du test de vérification E35 est positif.

Ce test est alors suivi par une étape E40 au cours de laquelle on modifie, la taille de la zone utilisable 110 de la mémoire physique EEPROM en fonction des valeurs des premier et deuxième bits (bit1, bit2) de l'ordre prédéterminé 210 reçu dans la commande 200.

Selon les différentes variantes de réalisations décrites précédemment en référence à la figure 1, cette étape E40 est réalisée, en créant, en détruisant le fichier FICHIER_VOID contenu dans la mémoire physique EEPROM, ou en modifiant la taille de ce fichier FICHIER_VOID.

L'étape E40 de modification de la taille de la zone utilisable 110 de la mémoire physique EEPROM est suivie par une étape E60 au cours de laquelle on mémorise le facteur multiplicateur de la fréquence de l'horloge externe CLOCK dans le registre mult_horl de la zone utilisable 110 de la mémoire EEPROM, ce registre étant lu par le processeur CPU à la mise sous tension pour paramétrer le composant PLL, ce qui a pour effet de modifier, de façon réversible la fréquence d'horloge de la carte.

Comme décrit précédemment, le facteur de multiplicateur de cette fréquence d'horloge est déterminé par la valeur du troisième bit bit3 et du quatrième bit bit4 de l'ordre 210 prédéterminé.

L'étape E60 de modification de la fréquence d'horloge est suivie par une étape E70 au cours de laquelle le processeur CPU écrit dans le registre soft de la mémoire non volatile EEPROM la valeur du cinquième bit bit5 de l'ordre 210.

Comme décrit précédemment, lorsque ce registre soft mémorise la valeur 1, une fonction logicielle f par exemple une fonction cryptographique

telle qu'une fonction de contrôle d'une signature de données numériques est rendue accessible en ce qu'elle peut être invoquée par un programme informatique mémorisé dans la mémoire ROM ou la mémoire EEPROM.

L'étape E70 est suivie par une étape E80 au cours de laquelle le processeur CPU mémorise dans le registre hard du circuit électronique 120 la valeur du sixième bit bit6 de l'ordre prédéterminé.

Lorsque ce registre hard mémorise la valeur 1, l'utilisation de ce circuit électronique 120 est autorisé. Dans le mode de réalisation préféré décrit ici, ce circuit électronique 120 est une unité cryptographique.

L'étape E80 est suivie par l'étape E20 de réception d'une commande déjà décrite.

REVENDICATIONS

1. Carte à microcircuit (100) comportant des moyens (RX) de réception d'une commande (200) et des moyens de modification d'au moins une performance de ladite carte sur réception de ladite commande, les moyens de modification étant caractérisés en ce qu'ils peuvent être mis en œuvre après une étape (E10) de personnalisation de ladite carte.

2. Carte à microcircuit selon la revendication 1, caractérisée en ce qu'elle comporte en outre des moyens d'authentification d'un émetteur de ladite commande (200).

3. Carte à microcircuit selon la revendication 2, caractérisée en ce que les moyens d'authentification comporte une clé d'authentification secrète.

4. Carte à microcircuit selon l'une quelconque des revendications 1 à 3, caractérisée en ce que les moyens de modification sont adaptés à déterminer ladite au moins une performance en fonction d'un ordre prédéterminé (210) reçu dans ladite commande (200).

5. Carte à microcircuit selon l'une quelconque des revendications 1 à 4, caractérisée en ce que lesdits moyens de réception (RX) sont adaptés à recevoir ladite commande (200) selon un protocole de type SMS.

6. Carte à microcircuit selon l'une quelconque des revendications 1 à 5, caractérisée en ce que lesdits moyens de modification d'au moins une performance sont adaptés à modifier la taille d'une zone utilisable (110) d'une mémoire physique (EEPROM) de ladite carte.

7. Carte à microcircuit selon la revendication 6, caractérisée en ce que ladite modification de la taille d'une zone utilisable (110) d'une mémoire physique (EEPROM) est effectuée en créant ou en détruisant au moins un fichier spécifique (FICHIER_VOID) compris dans ladite mémoire physique, ou en modifiant la taille d'au moins un fichier spécifique (FICHIER_VOID) compris dans ladite mémoire physique.

8. Carte à microcircuit selon l'une quelconque des revendications 1 à 7, caractérisée en ce que lesdits moyens de modification d'au moins une performance sont adaptés à modifier, de façon réversible ou non, une fréquence d'horloge de ladite carte.

9. Carte à microcircuit selon l'une quelconque des revendications 1 à 8, caractérisée en ce que lesdits moyens de modification d'au moins une performance sont adaptés à permettre ou empêcher, de façon réversible ou non, l'utilisation d'au moins une fonction logicielle (f) de ladite carte.

10. Carte à microcircuit selon l'une quelconque des revendications 1 à 9, caractérisée en ce que lesdits moyens de modification d'au moins une performance sont adaptés à permettre ou empêcher, de façon réversible ou non, l'utilisation de tout ou partie d'un circuit électronique (120) de ladite carte.

11. Carte à microcircuit selon la revendication 10, caractérisée en ce que ledit circuit électronique (120) est une unité cryptographique.

12. Carte à microcircuit selon l'une quelconque des revendications 1 à 11, caractérisée en ce qu'elle comporte en outre des moyens de synchronisation (130) adaptés à vérifier l'unicité de ladite commande (200).

13. Procédé de configuration d'une carte à microcircuit (100) caractérisé en ce qu'il comporte les étapes successives suivantes :

- personnalisation (E10) de ladite carte ;
- réception (E20) d'une commande (200) ; et
- modification (E40, E60, E70, E80) d'au moins une performance de la carte sur réception de ladite commande (200).

14. Procédé de configuration selon la revendication 13, caractérisé en ce que ladite étape de réception (E20) est suivie par une étape (E30) d'authentification d'un émetteur de ladite commande (200).

15. Procédé de configuration selon la revendication 13 ou 14, caractérisé en ce que, au cours de ladite étape de modification (E40, E60, E70, E80), on détermine ladite au moins une performance en fonction d'un ordre prédéterminé (210) reçu dans ladite commande (200).

16. Procédé de configuration selon l'une quelconque des revendications 13 à 15, caractérisé en ce que ladite étape (E20) de réception d'une commande (200) est conforme à un protocole de type SMS.

17. Procédé de configuration selon l'une quelconque des revendications 13 à 16, caractérisé en ce que, au cours de ladite étape (E40) de modification d'au moins une performance, on modifie la taille d'une zone utilisable (110) d'une mémoire physique (EEPROM) de ladite carte.

18. Procédé de configuration selon la revendication 17, caractérisé en ce que au cours de ladite modification de la taille d'une zone utilisable (110) d'une mémoire physique (EEPROM) , on crée ou on détruit au moins un fichier spécifique (FICHIER_VOID) compris dans ladite mémoire physique ou on modifie la taille d'au moins un fichier spécifique (FICHIER_VOID) compris dans ladite mémoire physique.

19. Procédé de configuration selon l'une quelconque des revendications 13 à 18, caractérisé en ce que, au cours de ladite étape (E60) de modification d'au moins une performance, on modifie, de façon réversible ou non, une fréquence d'horloge de ladite carte.

20. Procédé de configuration selon l'une quelconque des revendications 13 à 19, caractérisé en ce que, au cours de ladite étape (E70) de modification d'au moins une performance, on permet ou en empêche, de façon réversible ou non, l'utilisation d'au moins une fonction logicielle (f) de ladite carte.

21. Procédé de configuration selon l'une quelconque des revendications 13 à 20, caractérisé en ce que, au cours de ladite étape (E80) de modification d'au moins une performance, on permet ou en empêche, de façon réversible ou non, l'utilisation de tout ou partie d'un circuit électronique (120) de ladite carte.

22. Procédé de configuration selon la revendication 21, caractérisé en ce que ledit composant électronique (120) est une unité cryptographique.

23. Procédé de configuration selon l'une quelconque des revendications 13 à 22, caractérisé en ce qu'il comporte , préalablement à ladite étape (E40) de modification d'au moins une performance, une étape (E35) de vérification de l'unicité de ladite commande (200).

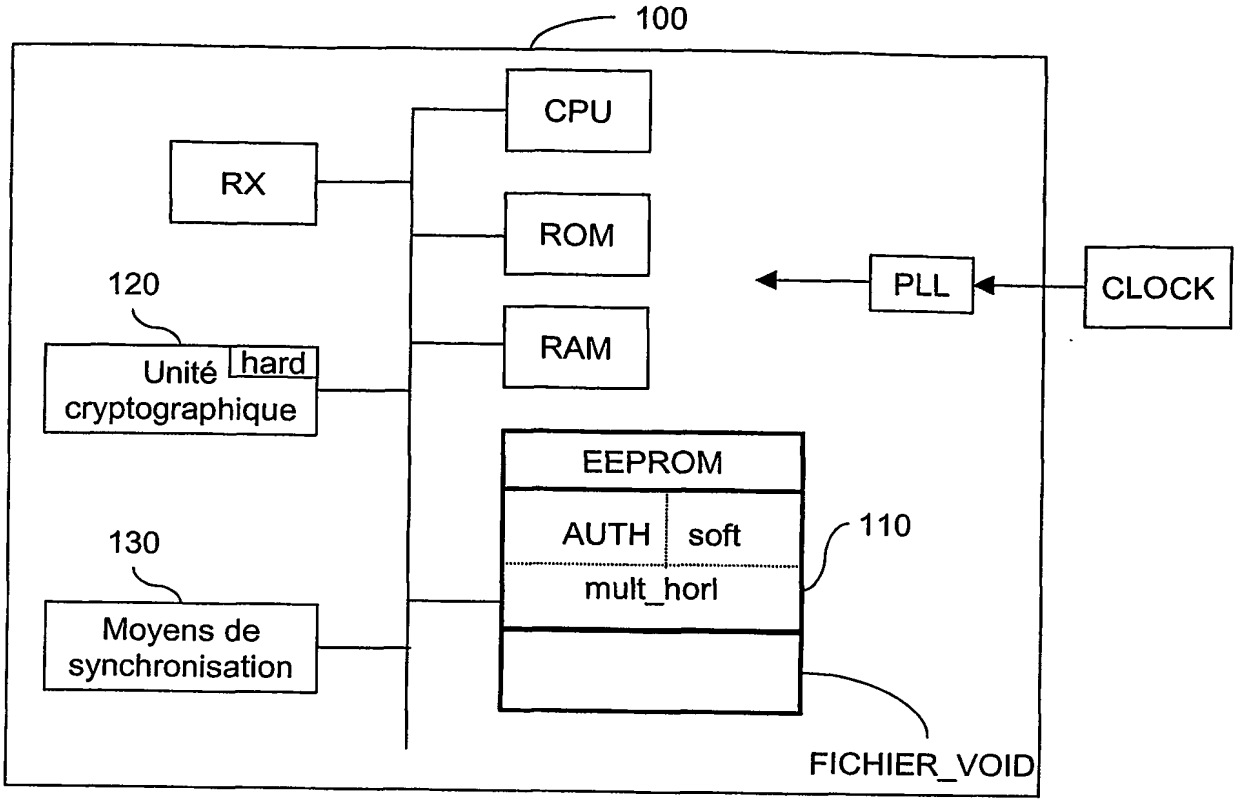


FIGURE 1

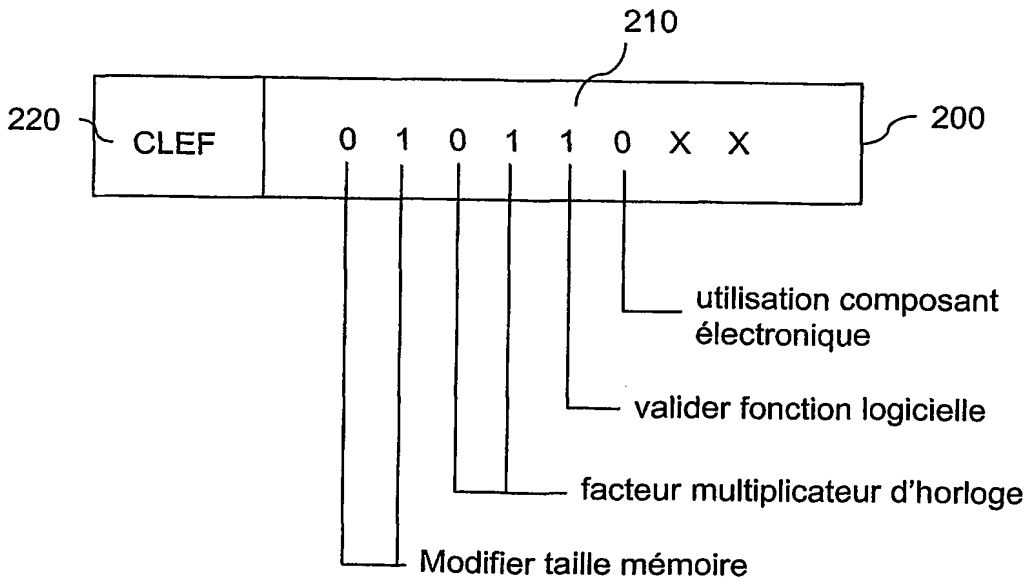


FIGURE 2

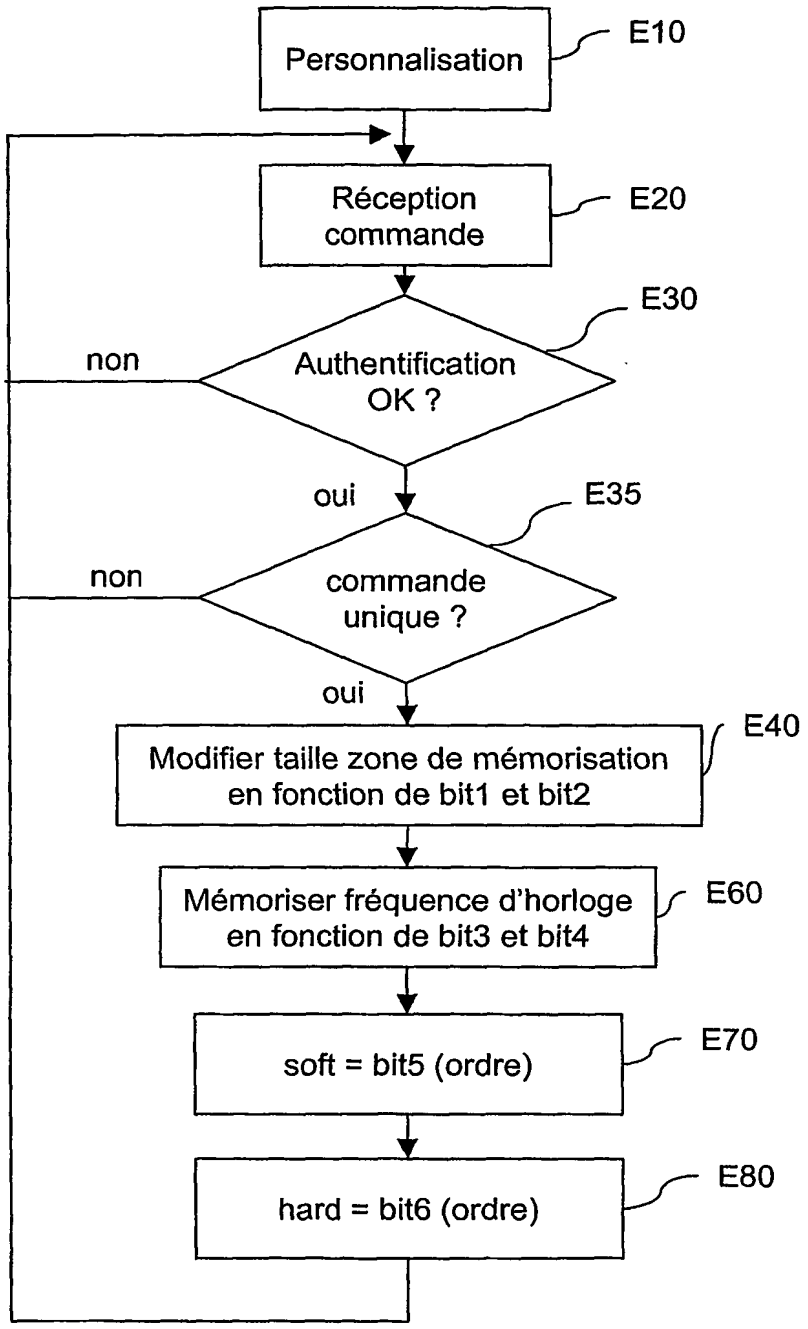

Personnalisation
E10
Réception commande
E20
E30
non
Authentification OK ?
oui
E35
non
commande unique ?
oui
Modifier taille zone de mémorisation en fonction de bit1 et bit2
E40
Mémoriser fréquence d'horloge en fonction de bit3 et bit4
E60
soft = bit5 (ordre)
E70
hard = bit6 (ordre)
E80

FIGURE 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT 03/02854

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K19/07

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 273 335 B1 (SLOAN JERRY F) 14 August 2001 (2001-08-14)	1,2,4, 9-11, 13-15,20
Y	column 2, line 63 -column 3, line 33	3,5,12
Y	EP 1 223 565 A (MOTOROLA INC) 17 July 2002 (2002-07-17) paragraphs '0004!,'0033!	12
Y	EP 1 143 688 A (CLIENT ELECTRONICS GMBH) 10 October 2001 (2001-10-10) paragraph '0007!	5

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 January 2004	09/02/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Koegler, L

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No
PCT/[redacted] 03/02854

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	RANKL; EFFING: "Handbuch der Chipkarten", CARL HANSER VERLAG , MÜNCHEN; WIEN XP002243893 ISBN: 3-446-21115-2 page 206-211 page 234-241, paragraph 5.6.5	1,6,7, 13,17,18
A	page 107	8
Y	EP 0 479 617 A (TOKYO SHIBAURA ELECTRIC CO) 8 April 1992 (1992-04-08) abstract; figure 6	3

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT 03/02854

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6273335 B1	14-08-2001	US 6179205 B1	30-01-2001
		AT 254322 T	15-11-2003
		AU 764621 B2	28-08-2003
		AU 2989199 A	20-09-1999
		CA 2321229 A1	10-09-1999
		DE 69912749 D1	18-12-2003
		EP 1060459 A1	20-12-2000
		WO 9945507 A1	10-09-1999
EP 1223565 A	17-07-2002	EP 1223565 A1	17-07-2002
EP 1143688 A	10-10-2001	EP 1143688 A1	10-10-2001
EP 0479617 A	08-04-1992	JP 4143881 A	18-05-1992
		DE 69129286 D1	28-05-1998
		DE 69129286 T2	08-10-1998
		EP 0479617 A2	08-04-1992
		US 5288978 A	22-02-1994

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT 03/02854

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06K19/07

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06K G07F H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 6 273 335 B1 (SLOAN JERRY F) 14 août 2001 (2001-08-14)	1,2,4, 9-11, 13-15,20
Y	colonne 2, ligne 63 -colonne 3, ligne 33	3,5,12
Y	EP 1 223 565 A (MOTOROLA INC) 17 juillet 2002 (2002-07-17) alinéas '0004!,'0033!	12
Y	EP 1 143 688 A (CLIENT ELECTRONICS GMBH) 10 octobre 2001 (2001-10-10) alinéa '0007!	5

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
29 janvier 2004	09/02/2004

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Koegler, L

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 03/02854

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
X	RANKL; EFFING: "Handbuch der Chipkarten" , CARL HANSER VERLAG , MÜNCHEN; WIEN XP002243893 ISBN: 3-446-21115-2 page 206-211 page 234-241, alinéa 5.6.5	1,6,7, 13,17,18
A	page 107	8
Y	EP 0 479 617 A (TOKYO SHIBAURA ELECTRIC CO) 8 avril 1992 (1992-04-08) abrégé; figure 6	3

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/03/02854

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 6273335	B1	14-08-2001	US	6179205 B1	30-01-2001
			AT	254322 T	15-11-2003
			AU	764621 B2	28-08-2003
			AU	2989199 A	20-09-1999
			CA	2321229 A1	10-09-1999
			DE	69912749 D1	18-12-2003
			EP	1060459 A1	20-12-2000
			WO	9945507 A1	10-09-1999
EP 1223565	A	17-07-2002	EP	1223565 A1	17-07-2002
EP 1143688	A	10-10-2001	EP	1143688 A1	10-10-2001
EP 0479617	A	08-04-1992	JP	4143881 A	18-05-1992
			DE	69129286 D1	28-05-1998
			DE	69129286 T2	08-10-1998
			EP	0479617 A2	08-04-1992
			US	5288978 A	22-02-1994